Copy to H.C.S.G. 22/9

15(9)

PRELIMINARY INTERROGATION OF REG. RAT

DR. Ferdinand VOEGELE (Chi Stelle, Ob.d.L.)

and Major Ferdinand FEICHTNER (O.C. of

LN Regt. 352, etc.)

Attached is the report on the initial interrogation of VOEGELE and FEICHTNER carried out on 12th September 1945, at Royal Victoria Patriotic School, Wandsworth, ("INKPOT") by F/Lt. V.E. Rolf, Captain I.M. Campbell, I.C., and Lt. LEVENSON, AUS.

Both prisoners appeared eager to divulge all the information they possessed on the subjects raised.

Also attached are copies of VOEGELE's subsequent homework, which he wrote in English.

FEICHTNER's homework will be issued separately.

TICOM

20 Sept. 1945 No. of pages 11

DISTRIBUTION

British

D.D.3
H,C.G.
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
C.C.R.
Lt. Col. Leathem
Cdr. Tandy
Major Morgan.

U.S.

Op-20-G (2) (via Lt.Cdr. Manson)
G-2 (via Lt.Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt.Col. Johnson)
Col. Lewis Powell, USSTAF

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Lt.Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. Cowan
Lt. Fehl
Ticom Files (4)

Additional

S.A.C. for Signals 5, Air Ministry 22/9
Lt. Levenson
G/Capt. Felkin, A.D.I. (K)
Prof. Norman.

PRELIMINARY INTERROGATION OF

Major Ferdinand FEICHTNER

R.R. Ferdinand VOEGELE.

QUESTIONNAIRE

1) Notes on career in GAF Sigint Service.
2) Detailed account of GAF Sigint Organisation in area or areas of which you have first hand knowledge.
3) Describe liaison with other Sigint Services.
4) Describe work done on:
   a) RAF 2 letter (Bomber Code).
   b) RAF 3 letter codes (Aircraft Reporting; Aircraft Movements).
   c) RAF Syko 9 or Rekoh).
   d) Middle East Aircraft Movements Code (5 letter pronounceable words).
   e) British High Grade Machine Cypher (5 letter).
   f) American High Grade Machine Cypher (5 letter).
   g) U. States Hagelin Machine M.209.
   h) Army Air Support Codes.
   i) Air/Ground Authentication Tables.
   j) Work on Russian Air Systems.
   k) Was work done on traffic of any other nations? Give details.
   l) RAF 4 figure cypher.
   m) Inter-departmental Cypher.
   n) Lettered Co-ordinates.
   o) British Met. Codes.

5) Mechanical aids employed in cryptanalysis, e.g. Hollerith Machinery, and details of use.
6) Describe GAF "Flying Y Service" - organisation, functions and measure of success attained.
7) Give details of:
   a) German Pulse receivers and their use by GAF Sigint units.
   b) Exploitation of Allied Radio and Radar aids to navigation.
      i) Ground.
      ii) Airborne.
   c) German Radio and Radar countermeasures. (Jamming, etc.)

HOMEWORK

Questions 1, 2, 3, 6 and 7 were set for Major Feichtner.

Questions 1, 2, 3 and 4 (k) (l) (m) and (o) were set for Dr. Voegele (Answers attached herewith, with the exception of 4 (m) which is still being written out by V.)

REMAINING QUESTIONS

4 (a) RAF 2 letter (Bomber Code)

Specimen pages were obtained from a crashed bomber in November or December, 1942. Within 14 days of this the code was being broken cryptographically. On an average 150 - 200 messages were intercepted daily. Sometimes traffic rose to 600 messages, 300 messages gave 50 to 60% of code. The initial break-in, each day, was via letters and numbers from messages containing spelling or giving indications of frequency changes.

4 (b) RAF 3 letter Codes

i) Aircraft Reporting Code

This, too, was broken regularly to an exploitable extent. Initial break-in was facilitated by:

a) "Returning to Base" with ETA.
b) Messages indicating frequency change.
c) Hourly broadcasts of barometric pressures.

There were 4 stations (one was Mt. Batten) in the Bristol Channel giving these hourly broadcasts which were extremely valuable because of i) the progressive change of pressure from hour to hour throughout the day and ii) the continuity provided from day to day. Weather information obtained from ARC messages permitted the breaking of UCO (Ground/Air Broadcast Weather Code). Sgt. Ruths last known to be at Husum with 7/355 , could give details.

ii) Aircraft Movements Code (U.K.)

Three-letter messages with serial numbers in clear and a repeated indicator were intercepted. Messages appeared to be exchanged between a U.K. station and a station on the borders of France and Belgium; the traffic was not broken but it was assumed that the messages dealt with supply matters.

4 (c) RAF Syko (or Rekoh)

In the early months of the war, January or February 1939, cards were badly constructed; sequencies of symbols were repeated, sometimes on as many as five lines of a card.

Usually all messages were being read by 3 or 4 pm. although cards were sometimes not complete before 7 or 8 pm. Middle East and Ferry Syko (or Rekoh) were both broken but content was of little or no value.

4.(d) Middle East Aircraft Movements Code (5-letter pronounceable words).

The first edition of the code was read; it was not strong enough for the encoding of what had previously been passed in self-evident code.

Messages were not read after the code was changed in May or June 1943. Messages were still being intercepted in 1944 since the volume of traffic made it possible to deduce the approximate number of aircraft arriving in the Mediterranean. Estimates were considered ridicul ous by the higher-ups.

4 (e) British High Grade Machine Cypher (5-letter)

Reg.rat Voegele volunteered the name "Typex" for this and stated that they had examined typex traffic in 1940 but had had no success at all with this and soon abandoned their efforts. He had never seen a typex machine but he had heard that a damaged machine was captured without drums. He assumed it was similar to the Enigma.

4 (f) American High Grade Cypher Machine (5 letter)

Voegele did not know the name of this machine and had no idea of its appearance or operating principle. As with Typex, no success was achieved and attempts to break the system were dropped.

4. (g) U.S. Hagelin Machine (M.209)

The first success was achieved in March or April, 1944. On the Western Front the keys were broken for 6 to 8 days per month but in the Mediterranean cypher discipline was much stronger and keys were broken on only one or two days per month.

A key chart was captured in September or October, 1944.

Although in theory 22 hours should suffice for breaking, the time lag was 8 to 10 days in practice, owing to delays in the reception of raw material.

The breaking of M.209 was soon left to the Army who intercepted most of the traffic. Hagelin traffic was considered of little value as compared with Slidex which was read in bulk. Lt. Zimmerlin (a French prisoner at Tuttlingen) and Sgt. von Metzen were M.209 specialists.

4 (h) Army Air Support Codes.

These were not broken but traffic evaluation plus knowledge of their own dispositions often served to indicate whether a target was accepted or refused.

4 (i) Air/Ground Authentication Tables.

No knowledge.

4.(j) Russian Air Systems.

Did not work on Russian Air Systems which were very simple.

Lt. von Lingen and Oberst von Werther were the Russian experts.

4 (n) Lettered Co-ordinates.

Broken without much difficulty. How?

5) Mechanical Aids Employed in Cryptanalysis.

Hollerith was extensively used for listing, sorting, differencing, etc.

No special machinery was employed but a 40 year old teleprinter which punched paper tape about 4 inches wide was considered to have possibilites as a "click" machine and a similar machine was on order from OKW. The idea was to punch messages up on tapes and discover depth by passing a moveable tape over a fixed tape. A light underneath would indicate when a large proportion of holes coincided.

OKW had a machine called the "Clock" (because it ticked when operating) employed for the attack on Strip Cypher. Voegele found it quicker to find repeats by the Hollerith method.

POINTS OF INTEREST NOT COVERED BY QUESTIONNAIRE.

1) Voegele stated that the primary object of interception was T/A and evaluation.

Cryptography was considered of secondary importance and consequently he was never allowed any say in the allocation of tasks for the intercept units. He frequently received 8 or 9 versions of the same message.

2) Other Middle East 5 letter Pronounceable Word Codes (R.R. Voegele)

None decoded. Didn't realise they were other than a/c movement messages. Words employed were identically the same.

3) Ploesti Raid (Major Feichtner)

They had been listening for some time to the heavy bombers practising for what later turned out to be the Ploesti raid. Just before the raid they heard one a/c say in clear over the R/T "Hope you have plenty of food aboard. We have a long journey ahead of us".

When the bombers left on the raid they kept W/T silence and followed the normal course for raids on Italy but when they changed course towards the Balkans their target became obvious to those familiar with their weeks of W/T and R/T practice. There was ample time to deploy fighters.

After the raid the number of aircraft letters missing from the W/T traffic served to amplify German estimates of casualties.

4) U.S. Telegraph Code.

Alphabetical code of 140,000 5 letter groups with discriminant TEIWA was introduced in October, 1943. Had recovered about 12000 items by May, 1944. By February, 1945, the traffic was being read currently.

5) Strip Cypher.

URSAL was the indicator of messages dealing with the Northern-route from the Summer of 1942 till December, 1943.

CENEB, the Southern route indicator, was introduced in June, 1942. This traffic was read in November, 1942. It was not read after the introduction of strip elimination but thought it could have been read on 200 messages a day.

6) Radio Teleprinter.

a) From April to October, 1944, clear radio T/P messages were intercepted regarding a/c movements between America and North Africa.
b) Similar messages in cypher with 6 letter indicators were also intercepted but these could not be read.

HOMEWORK.

VOEGELE, Ferdinand.

1) Career in Sigint Service.

From August 15th 1935 - Sept. 30th I received training in Morse, instruction in wireless communication, something about German cyphering systems, handling of Enigma and other obsolete German keys. This was at Kladow, West of Berlin.

From October 1935 until October 15th 1936 I was detached to Feste Funkempfangstelle des Heeres (Army Sigint Unit) at Stuttgart-Cannstatt (this period was interrupted by a two months military training at Air Base Kitzingen (Bavaria) in February and March 1936). At Stuttgart I had to do filing work, registering of names of French Air Bases and French Airforce Officers picked out from clear messages and French newspapers. Most of the time I had to translate French clear messages into German and decypher messages of an existing 3-figure code. This code was alphabetical and recyphered by letters changing 2 - 5 times a month. In summer 35 I began decrypting 4-figure messages of the Spanish Red Army, Caesar System.

On Oct. 15th I was detached to W.13 - Munich one of the new sigint stations of the Luftwaffe, where I translated French and Italian clear messages into German.

On January 1st, 37, I was ordered to Air Ministry Berlin, where the Chi.stelle was established consisting of about 10 men altogether. To me was entrusted decrypting. There was one other man who had to decypher Russian messages, but for all the other countries I was alone. During this year I decrypted Spanish messages. At the end of 37 and in 38 I had to begin decrypting of Czech messages, after having solved minor systems. I succeeded with the Czech Air Force Double Transposition cypher in summer 38. In September 38 Chi.stelle was transferred to Potsdam Wildpark (Marstall). There I began decrypting the French "Aviation Militaire" alphabetical 4 fig. system, recyphered by letters, which could be read in 39.

Back in Berlin in 39 I completed work on the aforesaid cypher and began a 4 fig. Yugoslav Cypher and British Government Telegraph Code which I got later on in photocopy from OKW. At the end of August 39 Chi.stelle was transferred where I was occupied till the end of July 1940 working on Syko, RAF 4 fig. and Interdepartmental Cypher.

End of July 40 decrypting of RAF 4 fig. was transferred to W.leit 3 at Bougival, La Celle St. Cloud near Paris and was there together with Syko till March 41, when my crew was transferred to W. 1 Ob.d.L. at Noisy, Asnieres sur Oise, where I had to stay till March 42. In 40 and 41 several decrypting crews were detached to 9/L.N.Rgt.40 at Taormina (Sicily), 8/L.N.Rgt.38 (Balkans, motorized) and W.14 (afterwards called W.3 Ob.d.L.) at Athens, W.22 (Husum) and W.Leit 2 and W.12 (Brussels) which crews I inspected many times.

At the end of 42 I was ordered back to Wildpark with a few men left behind in France for Syko. At Chi.stelle Marstall decrypting of USA Strip Cyphers, URSAL, C D A F, (Carib.Def.Air Force) and systems of Southern Route Indicator group CENEB etc. was done.

At the end of 42 most of the people from Athens where especially RAF 4 fig. was worked on were ordered back for work on the new RAF 4 fig. A Hollerith assembly was established at Marstall at the end of 42.

During 43 and 44 research work at Marstall was especially in USA strips, M.209, Slidex and Telwa with a crew of about 100 men, Hollerith included.

In February 1945 reduced personnel, many of them women, were transferred to 1/350 at Kressbronn, Bodensee.

As to myself I was an employee from 35 to 45, in June 40 I was granted the title of Regierungsrat. In summer 1943 I was offered the rank of Regierungsrat on active service but I did not accept. So I was Regierungsrat d.B.d.Lw.

2) Organisation of Chi-Stelle.

1937 FU-CHI 1 officer, 8-12 civilian employees

1938 " " 1 officer, 1 official, about 30 civilians

1939 2 officers, 2 officials, about 80 civilian employees.

Chi-Stelle
Chief Gst. Kohlmorgen

Ref. A	Ref.B	Ref.C	Ref.D	Ref.E
General	E V A L U A T I O N			DECRYPTING
Things	FRANCE	ENGLAND	RUSSIA	
Personnel	1943	1942	POLAND	
	D2 ENGLAND	C3-Brit.	CZECHS	
	B5 U.S.A.	MEDITERR.		

Ref. E

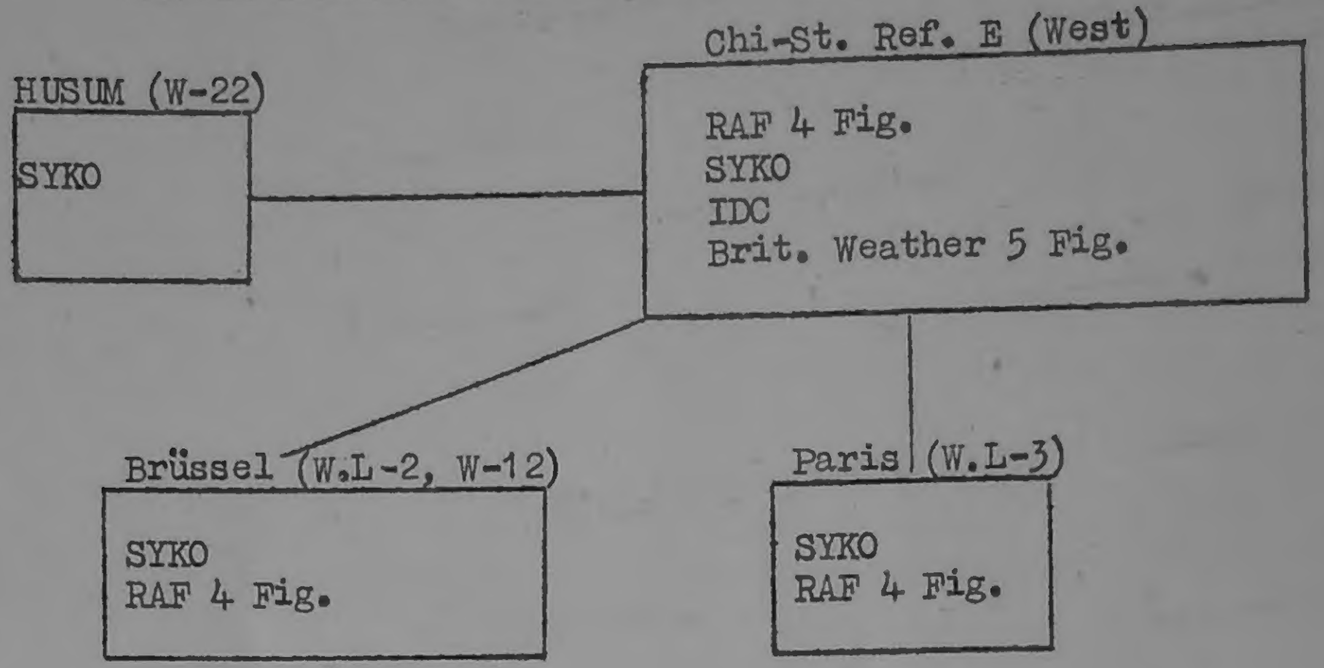
E_1 EAST (RUSSIA)	E_6 Hollerith	E_2 WEST (E_2 and E_3) British U.S.A.

Personnel of Ref. E September 1939 - 18-20!

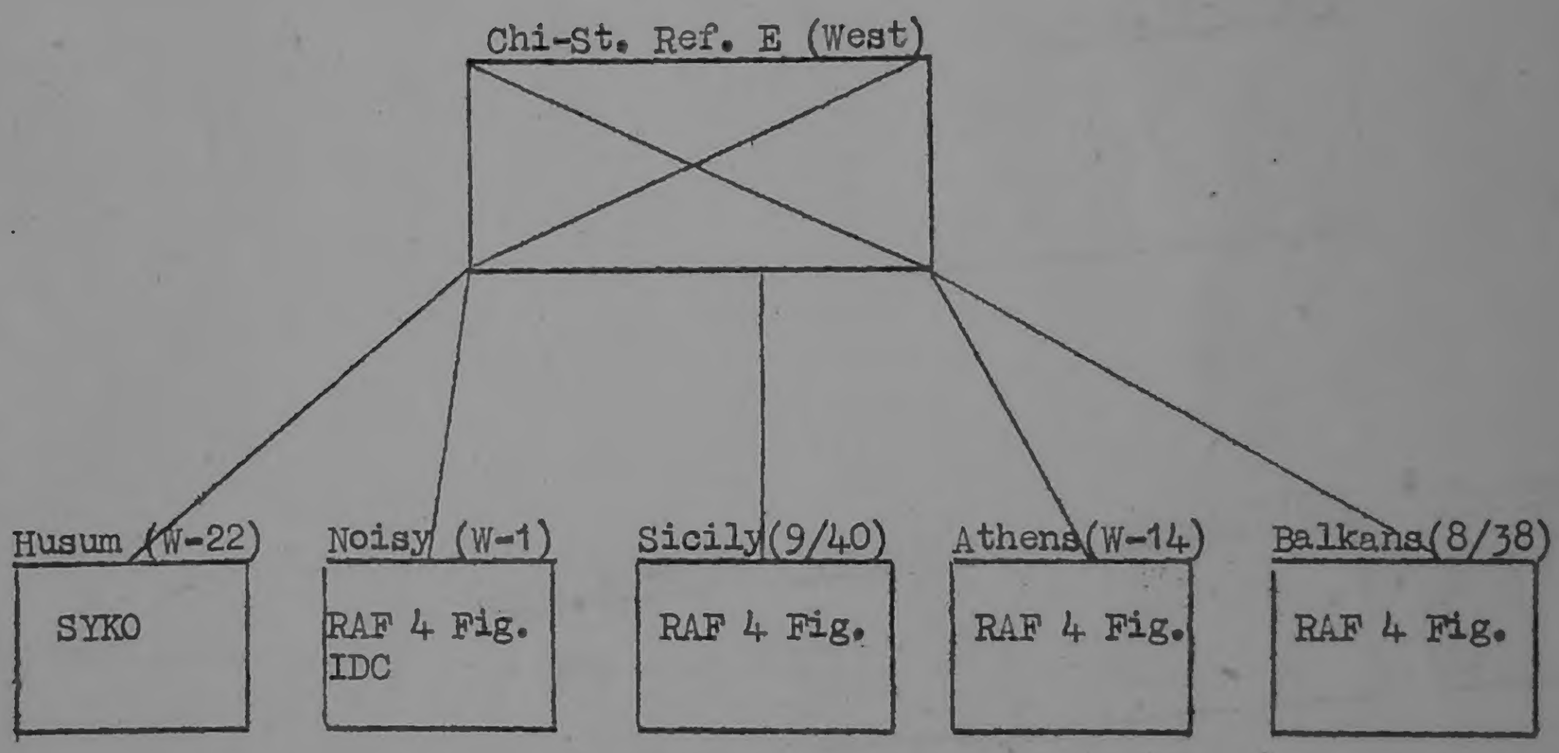
Summer 1940:	about	120	
1942	"	350	(West and EAST)
1944/45	"	250	(whereof about 100 women)

NOTE: From the fact that Evaluation ENGLAND, U.S.A., RUSSIA, each were Referat while Decrypting of all countries together was one Referat it is seen that decrypting was regarded as of secondary importance.

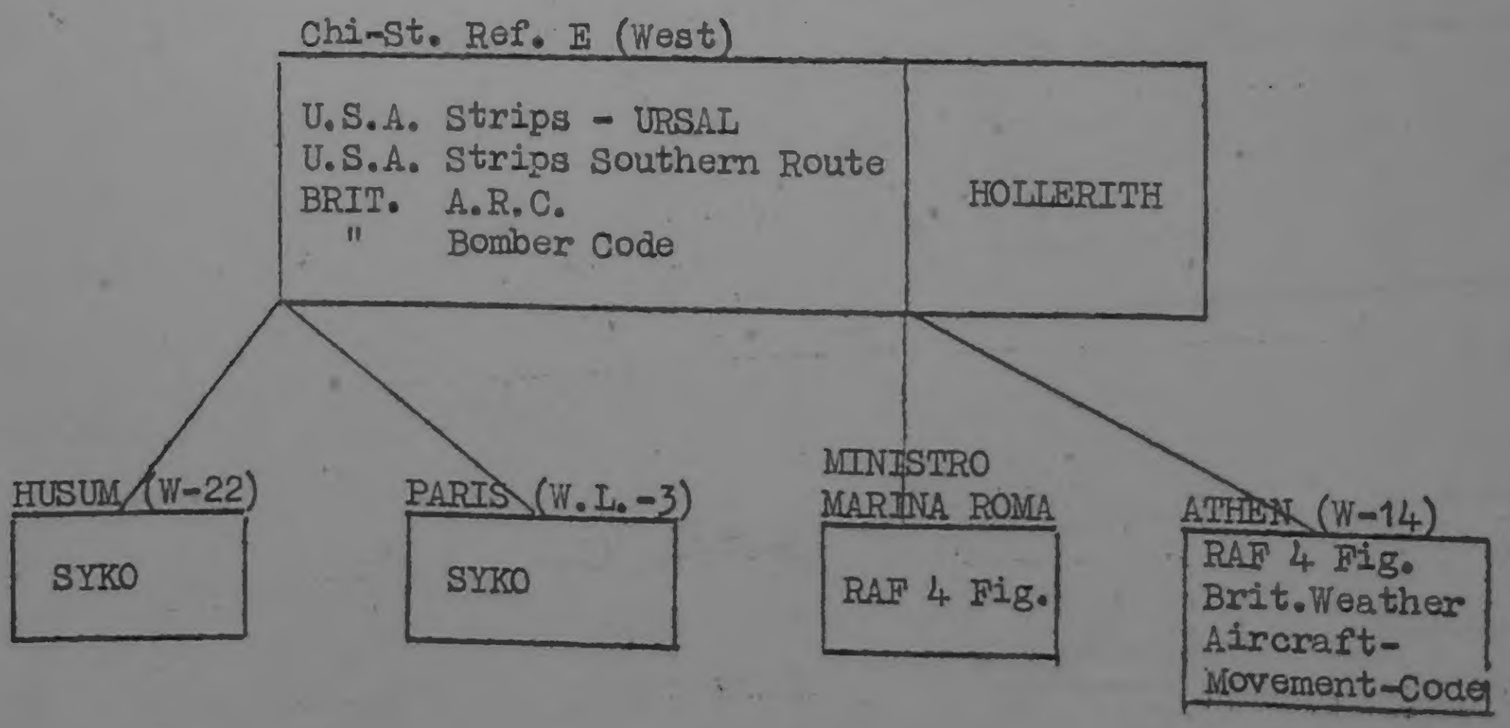
BRITISH SYSTEMS WORKED ON IN 1939/1940

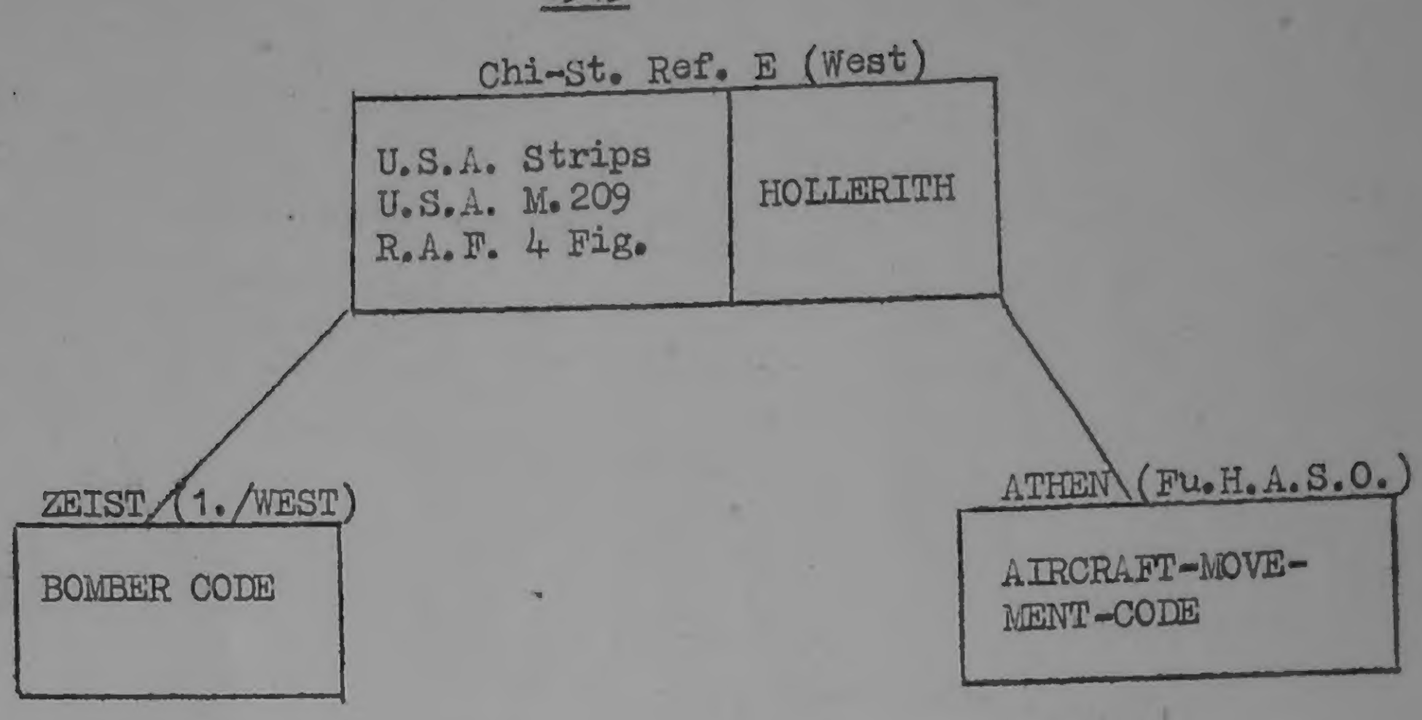


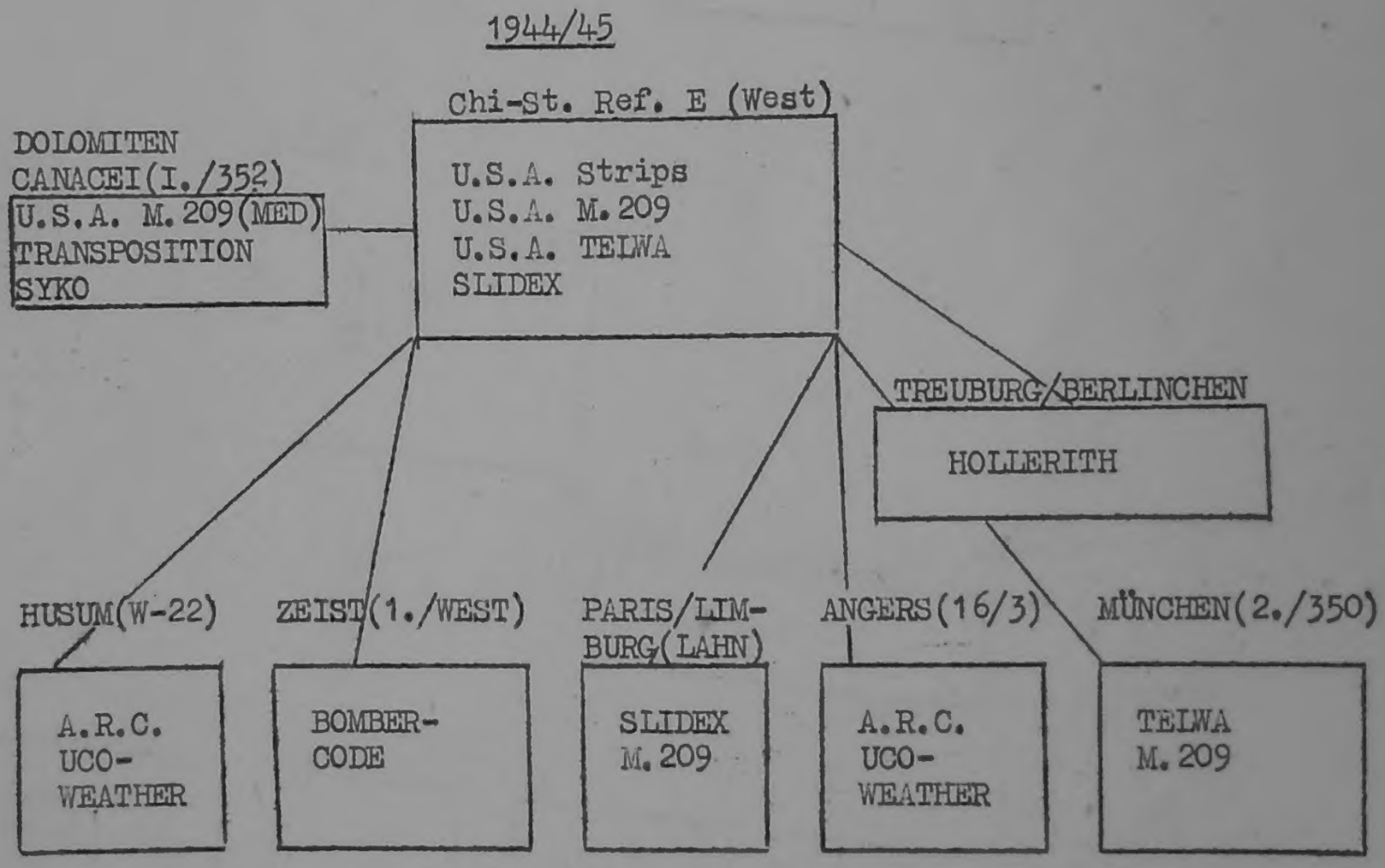
1941



1942 BRIT. AND U.S.A. SYSTEMS







3. Collaboration with other Decrypting Offices.

1940/42 Exchange of Recyphering book results (Austausch von errechneten Wurmphasen) for Interdepartmental Code with OKW, OKM and F.A. (Forschungsamt)

1942 5 Cryptographers were detached to Ministero Marina, Rome, for work on RAF 4 fig. Code.

1943 Interchange of U R S A L and C D A F with OKH.

1944/45 Collaboration with OKH (N A A S T 5) near Paris and later on near Limburg/Lahn regarding SLIDEX - M.209 - and U.S.A. Code T E L W A (Messages and Items of this latter Code were interchanged likewise with OKW Berlin. First two groups of intercepted M.209 messages were given to and received from OKM and OKH (Jueterbog)

VOEGELE, Ferdinand.

4 (k) Work done on systems other than British and U.S.A.

1935/36 French 3 cypher code, alphabetical recyphered by letters.

1936 Spanish cyphers, Caesar system, generally one letter represented by four 2 fig. groups, most of which to be reduced on disc systems.

1937 Czech Transposition, Exercise Tables.

1938 " Double Transposition

1938/39 French "Aviation Militaire" alphabetical 4 fig. Code recyphered by letters.

1939 Yugoslav 4 fig. Air Force Code, alphabetical, of about 500 items.

4 (l) Work done on RAF 4-figure cypher.

At the end of October, 1939, I began statistics of RAF 4 fig. on messages of Oct. 39 with a group of 20 soldiers who had not the slightest idea about decrypting - there was no time for teaching. Four weeks later I had the first items - 2222 take part 2, 1111, main code, 1584 from a.s.o. Shifting from relative numbers - for 2222 I had 9711 - 1111 was 0822 was done by 0983 = read following 5 figures in clear. I knew that the first digits of old non-comm. officers' Pay Book was 5 or 6, so I got the 5, the other digits I got by filling up figures with 000 for instance 0983 57643000. As a proof I found 5 messages dated December 24th (Xmas) which were sent in open code without recyphering. Further I got 2 messages sent in syko and repeated in RAF 4 fig. At the end of '40 some recyphering tables were completely reconstructed - 100 pages, each 20 lines, each line with five 4 fig. groups. In winter 1939/40 about 30% of these 4 fig. messages began with 2222. In January '41 many of the messages began with the text followed by address in brackets - so it was easier to find overlapping messages.

On April 1st code was changed. At first 2222 and 1111 were represented by one group only (at least practically), spelling being a = 01, b = 02, ... z = 26. After a fortnight I had the first 200 items of new code. Introduction of disguised Indicator group stopped work for someweeks. The 4 fig. decrypting group was brought to Athens and some weeks passed before decyphering was possible. From Sept. '41 to Nov. '42 the majority of the 200 - 400 daily intercepted 4 fig. messages could be decyphered with an average delay of 5 - 10 days, in single cases messages were decyphered the day of intercept. When in Nov.'42 a new code was brought into use attempts were without result - so messages and many of the crew were sent back to Marstall in March '43. At this time I myself was engaged in USA systems. In '43 and '44 the quantity of 4 fig. messages was less than 200 and even less than 100 a day. Many of them were General Recyphering Table, One Way system, Dummy and may be others. Messages of August '43 did not show the same characteristics as those of winter '42/43. At the end of '44 I made a new attempt with 4 fig. of 1944 on basis of differences between two 4 fig. groups. Result seemed possible in February '45 with at least 1,000 messages when reencyphered by table of 100 pages as before, or less with shorter books or single sheets for shorter periods. Details about this might be given by Unteroffizier Herbert RIEDEL, at last at 1/350 Kressbronn Bodensee, who in July '45 was French prisoner at Friedrichshafen (Bodensee) French Zone.

VOEGELE, Ferdinand.

4 (o) Decrypting of weather messages.

This was as a principle not the task of Chi-Stelle, Referat E.

1) After having succeeded in decrypting RAF 4 fig. cypher I was ordered to break the 5 fig. British Weather, preceded by a 5 letter group, of which 4 were consonants, the last letter eventually being a vowel. It was supposed to be a recyphered Copenhagen weather key. When I had succeeded in Spring 1940, this work was taken over by Chef Wetterdienst, Oberinspektor NAUMANN. In 1941/42 a new Weather decrypting station was established, Wenüb GLINDOW, Wetter Nachrichten Überwachungsstelle at GLINDOW near POTSDAM, Chief O.I. NAUMANN, which position he held till 1945. (It belonged to Z.W.G. (Zentrale Wetter Gruppe))

At times, when work of this unit was not satisfactory weather messages were decrypted by men of my crew at W.19 (= W.3 Ob.d.L. = LN.Rgt. Südost) from November 1941 to August 1943.

I remember that in summer 1944 Mr. NAUMANN told me that with allied messages indicator groups "Whist" and "South" he had no result. At that time he was interested in messages with address MURIA - LONDON sent by Swedish station(s), I had such messages early in 1940, but not later. Specialist for weather-decrypting of my crew was Lieutenant ZIMMERLIN, Karl, in April 1945 at 1/350 Krissbronn (Bodensee) where he was taken P.O.W. by 1st French Army, (studied meteorology).

2) There were many systems by which occasionally, many times daily weather reports were given, for instance:

i) SYKO, England until 1. July 1942, when weather was given in one way recyphering table system, interception of messages was stopped.

ii) SYKO, Mediterranean

iii) Bomber Code contained weather reports.

iv) Aircraft Reporting Code gave every hour the barometric pressure of four stations in Bristol Channel.

v) Alaco and UCO (plain) of the latter the values of barometric pressure were decyphered in 1944

vi) Air Warning Stations in Italy sent in 1944 simple transposition cypher weather messages which were decyphered.